(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 08018582 A

(43) Date of publication of application: 19 . 01 . 96

(51) Int. Cl H04L 12/40
H04L 12/46
H04L 12/28

(21) Application number: 06149722

(22) Date of filing: 30 . 06 . 94

(71) Applicant: TOSHIBA CORP

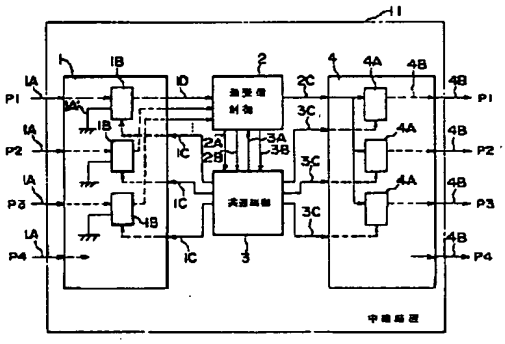
(72) Inventor: ANDO ARATA

(54) NETWORK REPEATER AND NETWORK SYSTEM USING IT

(57) Abstract:

PURPOSE: To prevent the use of the network by an illegal terminal equipment by applying enable/disable control to each port as required.

CONSTITUTION: A network repeater 11 has a reception enable/disable circuit 1B respectively provided corresponding to ports P1-P4, and a transmission enable/disable circuit 4A and the transmission or reception of the circuits is subject to enable/disable control by a command from a terminal equipment. When, for example, a manager of the network or the like finds out the existence of an illegal terminal equipment by monitoring a terminal equipment address or protocol on the network, the reception of the port corresponding to the network in which the illegal terminal equipment is in existence is inhibited.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平８－１８５８２

(43)公開日　平成８年（１９９６）１月１９日

(51)Int.Cl.[6]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
H04L 12/40				
12/46				
12/28				
			H04L 11/00	320
				310　C

審査請求　未請求　請求項の数３　ＯＬ　（全７頁）

(21)出願番号　特願平６－１４９７２２

(22)出願日　平成６年（１９９４）６月３０日

(71)出願人　０００００３０７８
株式会社東芝
神奈川県川崎市幸区堀川町７２番地

(72)発明者　安東　新
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内

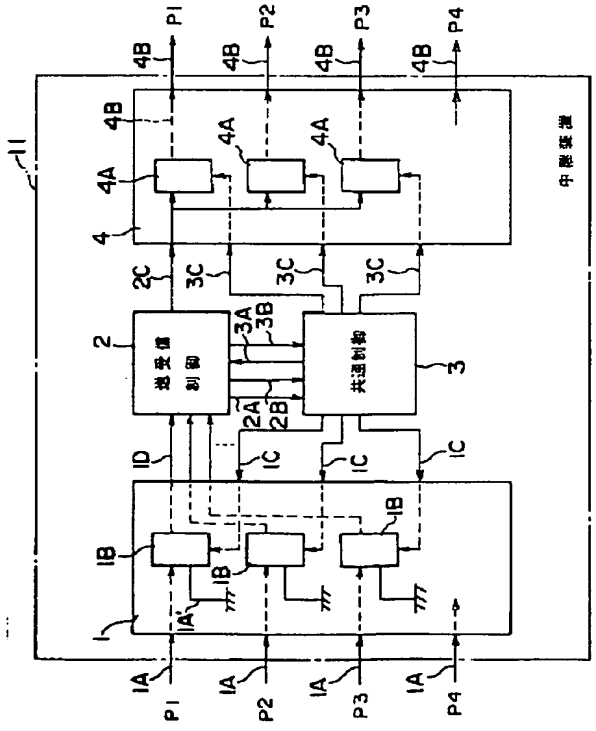
(74)代理人　弁理士　鈴江　武彦

(54)【発明の名称】ネットワーク中継装置およびこれを使用したネットワークシステム

(57)【要約】

【目的】各ポートを必要に応じてイネーブル／ディスエーブル制御できるようにして、不正端末によるネットワーク使用の防止を実現する。

【構成】ネットワーク中継装置１１は、ポートＰ１～Ｐ４にそれぞれ対応して設けられた受信イネーブル／ディスエーブル回路１Ｂ、および送信イネーブル／ディスエーブル回路４Ａを有しており、これら回路は端末からのコマンドによってその送信動作または受信動作がイネーブル／ディスエーブル制御される。このため、例えばネットワークの管理者などが、ネットワーク上の端末アドレスやプロトコルの監視によって不正端末の存在を発見した場合には、その不正端末が存在するネットワークに対応するポートの受信動作などを禁止することができる。



1

【特許請求の範囲】

【請求項１】　ネットワークにそれぞれ接続される複数のポートを有し、それらポート間のデータ転送によってネットワークを相互接続するネットワーク中継装置において、

前記ポート毎に設けられた複数の送受信装置と、

外部からのコマンドを受信し、そのコマンドに応じて前記複数の送受信装置の送信または受信動作をポート毎に個別に許可／禁止するポート制御手段とを具備することを特徴とするネットワーク中継装置。

【請求項２】　ネットワークにそれぞれ接続される複数のポートを有し、それらポート間のデータ転送によってネットワーク間を相互接続するネットワーク中継装置において、

前記ポート毎に設けられた複数の送受信装置と、

外部からのコマンドを受信し、そのコマンドに応じて前記複数の送受信装置の送信または受信動作をポート毎に個別に許可／禁止するポート制御手段と、

受信動作が禁止されたポートに供給されるデータの送信元アドレスと予め登録された端末のアドレス情報とを比較し、一致した際に該当する送受信装置の受信動作の禁止を解除する受信禁止解除手段とを具備することを特徴とするネットワーク中継装置。

【請求項３】　ネットワーク上の端末から他のネットワーク上の端末へのデータ転送経路が複数設定できるように相互接続された複数のネットワーク中継装置を具備するネットワークシステムであって、

前記各ネットワーク中継装置は、

ネットワークに接続される複数のポートと、

前記ポート毎に設けられた複数の送受信装置と、

外部からのコマンドを受信し、そのコマンドに応じて前記複数の送受信装置の送信または受信動作をポート毎に個別に許可／禁止するポート制御手段とを具備し、

送信元端末から送信先端末へのデータ転送経路を任意に設定できるようにしたことを特徴とするネットワークシステム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】この発明は、サーバ、ブリッジ、ルータ、またはゲートウェイ等のネットワーク中継装置、およびそのネットワーク中継装置を使用したネットワークシステムに関する。

【０００２】

【従来の技術】一般に、複数のＬＡＮ（ローカルエリアネットワーク）やＷＡＮ（ワイドエリアネットワーク）を相互に接続する方式として、ブリッジ、ルータ、ゲートウェイ等のネットワーク中継装置が知られている。

【０００３】これら各ネットワーク中継装置は、ネットワークセグメントに接続される複数のポートを有しており、それらポート間で受信パケットの転送を行うことによってネットワークセグメントを相互接続する。ポート間の転送は次のようなフィルタリング処理によって行われる。

2

【０００４】例えば、第１および第２の２つのポートを有するブリッジ装置が第１ポートでパケットを受信した時には、その受信したパケットの宛先アドレスによって指定されるデータステーションが接続されているポートが調べられ、そのポートに受信パケットが転送される。もしそのポートが受信ポートであれば、受信パケットは廃棄される。

【０００５】このようなネットワーク中継装置においては、ネットワークシステムの安全性を確保するために、次のようなポート制御が行われている。すなわち、ネットワークに接続されたあるデータステーションが故障し、それがデータ送信し続けことによってネットワーク全体に影響が及ぶことを防止するために、ネットワーク中継装置は、ある一定以上のデータ長を検出した場合、そのポートを論理的に切り離す機能を有している。

【０００６】また、信号／衝突検出型のネットワークでは、ある単位時間中に所定回数以上の衝突を検出した場合に、該当するポートを切り離す機能を持つ中継装置もある。

【０００７】しかしながら、このような従来のポート制御機能は、ある特定の信号の送受信状態が発生した時に自動的に働くいわゆる障害対策としての機能に過ぎず、正常なプロトコルでデータ送受信が行なわれている限りは何等ポート制御を行うことはできない。

【０００８】このため、ネットワーク上に不正端末が存在することが発見された場合であっても、その不正端末が正常な手続きでアクセス動作している限りはポート制御機能は働かない。したがって、不正端末によるネットワークアクセスを防止することはできなかった。

【０００９】また、従来のネットワークの形態は、バス、スター、リングの組み合わせでのみ可能であり、一部のネットワークが故障した場合の迂回路形成等が困難であった。

【００１０】

【発明が解決しようとする課題】従来のポート制御機能は、ある特定の信号の送受信状態が発生した時に自動的に働くいわゆる障害対策としての機能に過ぎず、正常なプロトコルでデータ送受信が行なわれている限りは何等ポート制御を行うことはできなかった。このため、必要に応じてポートを動的に制御する事ができず、不正端末によるネットワーク使用の防止や、障害発生時の迂回路設定などを行うことができない欠点があった。

【００１１】この発明はこの様な点に鑑みてなされたもので、各ポートを必要に応じてイネーブル／ディスエーブル制御できるようにして、不正端末によるネットワーク使用の防止や、障害発生時の迂回路設定などを行うことができるネットワーク中継装置を提供することを目的

とする。

【００１２】

【課題を解決するための手段および作用】この発明は、ネットワークにそれぞれ接続される複数のポートを有し、それらポート間のデータ転送によってネットワークを相互接続するネットワーク中継装置において、前記ポート毎に設けられた複数の送受信装置と、外部からのコマンドを受信し、そのコマンドに応じて前記複数の送受信装置の送信または受信動作をポート毎に個別に許可／禁止するポート制御手段とを具備することを特徴とする。

【００１３】このネットワーク中継装置においては、外部からのコマンドによって任意のポートの送信動作または受信動作をイネーブル／ディスエーブル制御することができる。このため、例えばネットワークの管理者などが、ネットワーク上の端末アドレスやプロトコルの監視によって不正端末の存在を発見した場合には、その不正端末が存在するネットワークに対応するポートの受信動作などをコマンドによって禁止することができる。

【００１４】また、この発明は、ネットワークにそれぞれ接続される複数のポートを有し、それらポート間のデータ転送によってネットワーク間を相互接続するネットワーク中継装置において、前記ポート毎に設けられた複数の送受信装置と、外部からのコマンドを受信し、そのコマンドに応じて前記複数の送受信装置の送信または受信動作をポート毎に個別に許可／禁止するポート制御手段と、受信動作が禁止されたポートに供給されるデータの送信元アドレスと予め登録された端末のアドレス情報とを比較し、一致した際に該当する送受信装置の受信動作の禁止を解除する受信禁止解除手段とを具備することを特徴とする。

【００１５】このネットワーク中継装置においては、受信動作が禁止されたポートに供給されるデータの送信元アドレスが予め登録されたアドレス情報と一致する場合には受信動作が許可されるように構成されており、不正端末以外の他の端末の送受信に影響を与えること無く、不正端末のネットワークアクセスだけを防止することができる。

【００１６】また、この発明は、ネットワーク上の端末から他のネットワーク上の端末へのデータ転送経路が複数設定できるように相互接続された複数のネットワーク中継装置を具備するネットワークシステムであって、前記各ネットワーク中継装置は、ネットワークに接続される複数のポートと、前記ポート毎に設けられた複数の送受信装置と、外部からのコマンドを受信し、そのコマンドに応じて前記複数の送受信装置の送信または受信動作をポート毎に個別に許可／禁止するポート制御手段とを具備し、送信元端末から送信先端末へのデータ転送経路を任意に設定できるようにしたことを特徴とする。

【００１７】このネットワークシステムにおいては、複数のネットワーク中継装置を例えばメッシュ状に結合することにより複数のデータ転送経路が設けられており、通常は、ある端末間の経路がポイントツーポイントとなるようにポートのイネーブル／ディスエーブル制御を行っておき、障害発生やトラフィック状態に応じてその経路を動的に変更するといった運用が可能になる。

【００１８】

【実施例】以下、図面を参照してこの発明の実施例を説明する。図１にはこの発明の一実施例に係わるネットワーク中継装置を用いたネットワークシステムの構成が示されている。ネットワーク中継装置１１は２以上のポートを持つマルチポートタイプの中継装置であり、ここでは、ネットワーク中継装置１１が図示のように４つのポートＰ１～Ｐ４を持ち、それらポートＰ１～Ｐ４がそれぞれＬＡＮセグメント１２～１５に接続されている場合を例示して説明する。

【００１９】ＬＡＮセグメント１２～１５の各々には、データ処理端末が接続されている。これらデータ処理端末は、ワークステーションやパーソナルコンピュータ、またはミニコンピュータ等によって実現されるものであり、対応するＬＡＮセグメントを介して相互に通信を行うと共に、ネットワーク中継装置１１を介して他のＬＡＮセグメント上のデータ処理端末などと通信を行う。

【００２０】ネットワーク中継装置１１は、例えば、ネットワークサーバ、リピータ、ブリッジ、ルータ、またはゲートウェイ等を構成するものであり、ＬＡＮセグメント１２～１５間の相互接続、またはＷＡＮ、公衆回線網等に接続するため等に使用される。

【００２１】このネットワーク中継装置１１は、ポートＰ１～Ｐ４を個別にイネーブル／ディスエーブル制御するためのポートイネーブル／ディスエーブル制御ユニット１１１を備えている。ポートイネーブル／ディスエーブル制御ユニット１１１は、斜線で図示されているＬＡＮセグメン上の遠隔端末や、またはネットワーク中継装置１１に直接接続された管理装置などからの要求に応じて、４つのポートＰ１～Ｐ４それぞれの受信動作および送信動作を個別に制御する事ができる。

【００２２】次に、図２を参照して、ネットワーク中継装置１１の具体的な構成の一例を説明する。ネットワーク中継装置１１は、図示のように、受信部１、送受信制御部２、共通制御部３、および送信部４を備えている。

【００２３】受信部１はポートＰ１～Ｐ４それぞれからのパケット受信データ１Ａを受信するためのものであり、ポートＰ１～Ｐ４にそれぞれ対応して設けられた４つの受信データイネーブル／ディスエーブル回路１Ｂを有している。

【００２４】これら４つの受信データイネーブル／ディスエーブル回路１Ｂは、それぞれ対応するポートＰ１～Ｐ４からパケットデータ１Ａを受信する回路であり、イネーブル／ディスエーブル信号１Ｃによってその受信動

作が個別に許可／禁止されるように構成されている。

【００２５】すなわち、受信データイネーブル／ディスエーブル回路１Ｂはイネーブルの時には受信データ１Ａを選択し、ディスエーブルの場合には接地電位１Ａ´を選択する。これら４つの受信データイネーブル／ディスエーブル回路１Ｂからの受信データ出力１Ｄは、送受信制御部２に共通に供給される。

【００２６】送信部４は、ポートＰ１～Ｐ４それぞれからパケットデータ４Ｂを送信するためのものであり、ポートＰ１～Ｐ４にそれぞれ対応して設けられた４つの送信データイネーブル／ディスエーブル回路４Ａを有している。これら４つの送信データイネーブル／ディスエーブル回路４Ａは、それぞれ対応するポートＰ１～Ｐ４からパケットデータ４Ｂを送信するために設けられた回路であり、イネーブル／ディスエーブル信号３Ｃによってその受信動作が個別に許可／禁止されるように構成されている。

【００２７】４つの送信データイネーブル／ディスエーブル回路４Ａには、送受信制御部２からの送信データが共通に供給され、相手先端末に対応するポートに対応する送信データイネーブル／ディスエーブル回路４Ａから出力される。

【００２８】送受信制御部２は、受信データイネーブル／ディスエーブル回路１Ｂから受信した受信データの制御、および送信データイネーブル／ディスエーブル回路４Ａに出力する送信データの制御を行うためのものであり、通常、クロックリカバリ回路、ＦＩＦＯバッファ、メモリなどから構成される。また、送受信制御部２は、受信データイネーブル／ディスエーブル回路１Ｂの制御のために、受信データ２Ａ、および受信クロック２Ｂを利用して、共通制御３に受信したコマンドなどを送信する。

【００２９】共通制御部３は、受信データイネーブル／ディスエーブル回路１Ｂ、および送信データイネーブル／ディスエーブル回路４Ａをイネーブル／ディスエーブル制御するためのものであり、送受信制御部２から転送されるコマンドに応じて動作する。

【００３０】この共通制御部３は、通常、シリアルコントローラ、データシリアル／パラレル変換回路、ＣＰＵ、メモリなどから構成される。また、３４Ａ，３Ｂは共通制御部３が送受信制御部２との通信にしようするデータ、クロックなどである。

【００３１】次に、図２の中継装置１１の動作を説明する。通常のデータ転送時においては、各ポートの受信イネーブル／ディスエーブル回路１Ｂは制御信号１Ｃによって受信データ１Ａを選択するイネーブル状態に設定されている。また、各ポートの送信イネーブル／ディスエーブル回路４Ａも制御信号３Ｃにより送信イネーブル状態に設定されている。

【００３２】ここで、ネットワークの管理者などが別途

ネットワークに接続された装置、または中継装置１１の持つ機能などによって、ネットワーク上に不正端末の存在を発見した場合、または障害／トラフィックに応じてあるポートのイネーブル／ディスエーブル制御により経路を変更したい場合を考える。

【００３３】この場合、ネットワーク管理者は、ネットワーク１３上の所定の端末などを利用して、中継装置１１に対してコマンドを発行し、イネーブル／ディスエーブルするポート番号などを通知する。

【００３４】この時、ポートＰ２から受信した中継装置１１宛のコマンドは送受信制御部２を経由して共通制御部３に入力される。共通制御部３は、受信コマンドを解析し、それが上記コマンドであった場合には、受信制御信号１Ｃまたは送信制御信号３Ｃ、あるいはそれら両方の制御信号を用いて、送受信のイネーブル／ディスエーブル制御を行う。

【００３５】コマンドによってポートＰ１の受信動作をディスエーブルすることが指定されると、受信部１においては、制御信号１Ｃにより受信イネーブル／ディスエーブル回路１Ｂの入力を受信データ１Ａから１Ａ´に切り替えられ、その受信動作が禁止される。

【００３６】この構成においては、端末からコマンドなどによって任意のポートの送信動作または受信動作をイネーブル／ディスエーブル制御することができる。このため、例えばネットワークの管理者などが、ネットワーク上の端末アドレスやプロトコルの監視によって不正端末の存在を発見した場合には、その不正端末が存在するネットワークに対応するポートの受信動作などを禁止することができ、ネットワークの信頼性の向上を図る事ができる。

【００３７】次に、図３を参照して、受信イネーブル／ディスエーブル回路１Ｂ周辺の他の回路構成を説明する。すなわち、この図３においては、図２の構成に加え、各ポート毎にシリアル／パラレル変換回路１Ｅ、パラメータレジスタ１Ｆ、および復旧回路１Ｉを備えている。

【００３８】シリアル／パラレル変換回路１Ｅは、受信イネーブル／ディスエーブル回路１Ｂと並列に設けられており、受信イネーブル／ディスエーブル回路１Ｂのイネーブル／ディスエーブル状態に関係なく受信データ１Ａを受信し、それをシリアルデータからパラレルデータに変換し、パラメータレジスタ１Ｆの設定値と比較する。この比較動作は、受信データの送信元アドレスが、パラメータレジスタ１Ｆに予め設定された受信許可端末のアドレスと一致するか否かを検出するために行われる。

【００３９】復旧回路１Ｉは、制御信号１Ｃにより受信ディスエーブルが宣告されていても、シリアル／パラレル変換回路１Ｅから一致検出信号１Ｈが発生された時には受信イネーブル／ディスエーブル回路１Ｂをイネーブ

ル状態に設定する回路である。

【００４０】すなわち、この図３の構成においては、例えばポートＰ１が受信ディスエーブルの場合においては、制御信号１Ｃ（図３では１Ｊ）により受信データ１Ａは無視され、１Ｄには受信データは出力されない。しかし、この状態に於いても、受信データ１Ａは常にシリアル／パラレル変換回路１Ｅにて受信されており、その送信元アドレス（または、送信先アドレスなど）のモニタが行われている。予め登録された各端末の物理アドレスはレジスタ１Ｆに設定されており、シリアル／パラレル変換回路１Ｅのアドレス値と常に比較される。

【００４１】両者が合致した場合には、信号１Ｈにてアドレスの一致が復旧回路１Ｉに通知され、仮に共通制御部３から受信ディスエーブル信号１Ｃ（ここでは、１Ｃ２）が発生されていても、復旧回路１Ｉは正当な端末からのデータであると判断し、受信イネーブル／ディスエーブル回路１Ｂをイネーブル状態に切り替える。

【００４２】この場合、受信イネーブル／ディスエーブル回路１Ｂの受信データの先頭がカットされる危険があるので、ディスエーブル状態であっても受信データを保持するバッファを受信イネーブル／ディスエーブル回路１Ｂに設けるなどの手法を採用する事が好ましい。この場合、その受信バッファの内容はポートがイネーブルであれば読み出され、ディスエーブルであれば読み出されない。

【００４３】この構成においては、受信動作が禁止されたポートに供給されるデータの送信元アドレスが予め登録されたアドレス情報と一致する場合には受信動作が許可されるように構成されているので、不正端末以外の他の端末の送受信に影響を与えること無く、不正端末のネットワークアクセスだけを防止することができる。

【００４４】次に、図４を参照して、図２または図３の構成を持つネットワーク中継装置１１を用いたネットワークシステムの構築例を説明する。このネットワークシステムにおいては、複数のネットワーク中継装置１１がＬＡＮセグメントを介してメッシュ状に結合されており、これによって、あるＬＡＮセグメント上の端末から他のＬＡＮセグメント上の端末までのデータ転送経路が複数設定されるようになっている。

【００４５】この場合、通常は、ある端末間の経路がポイントツーポイントとなるようにポートのイネーブル／ディスエーブル制御を行っておき、障害発生やトラフィック状態に応じて、コマンドによるポートのイネーブル／ディスエーブル制御を行ってその経路を自動的または人為的に変更するといった運用を行うことが可能になる。

【００４６】

【発明の効果】以上のように、この発明によれば、各ポートを必要に応じてイネーブル／ディスエーブル制御できるようになり、不正端末によるネットワーク使用の防止や、障害発生時の迂回路設定などを行うことが可能となる。

【図面の簡単な説明】

【図１】この発明の一実施例に係わるネットワーク中継装置を用いたネットワークシステムの構成を示すブロック図。

【図２】図１に示したネットワーク中継装置の具体的構成の一例を示すブロック図。

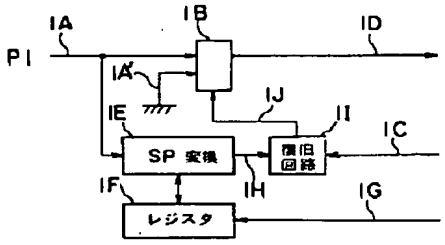
【図３】図１に示したネットワーク中継装置の他の具体的構成の一例を示すブロック図。

【図４】図１のネットワーク中継装置を多数用いて構成したネットワークシステムの一例を示す図。

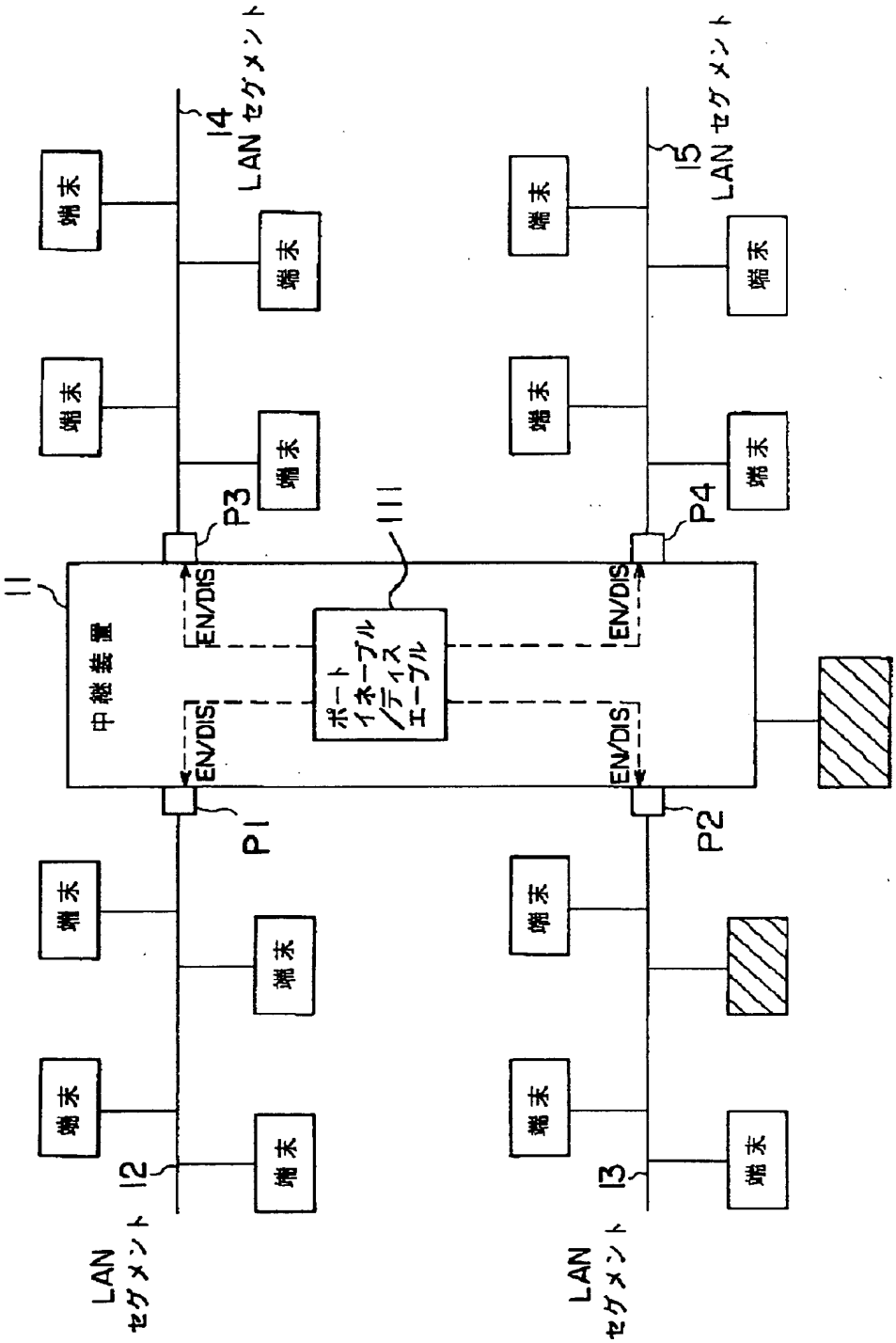
【符号の説明】

１…受信部、１Ｂ…受信イネーブル／ディスエーブル回路、１Ｅ…シリアル／パラレル変換回路、１Ｆ…パラメータレジスタ、１Ｉ…復旧回路、２…送受信制御部、３…共通制御部、４…受信部、４Ａ…送信イネーブル／ディスエーブル回路、１１…ネットワーク中継装置、１２，１３，１４，１５…ＬＡＮセグメント、Ｐ１，Ｐ２，Ｐ３，Ｐ４…ポート。

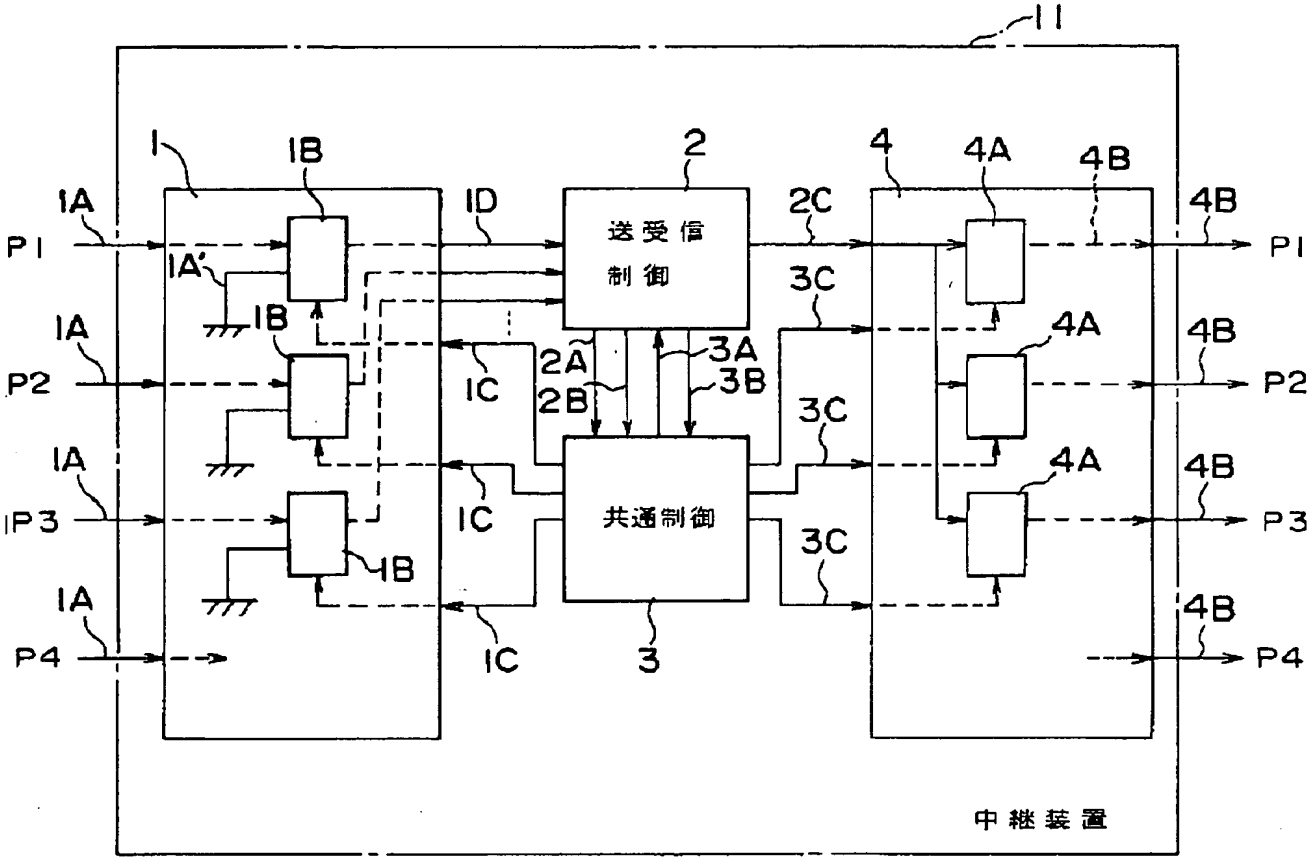
【図３】



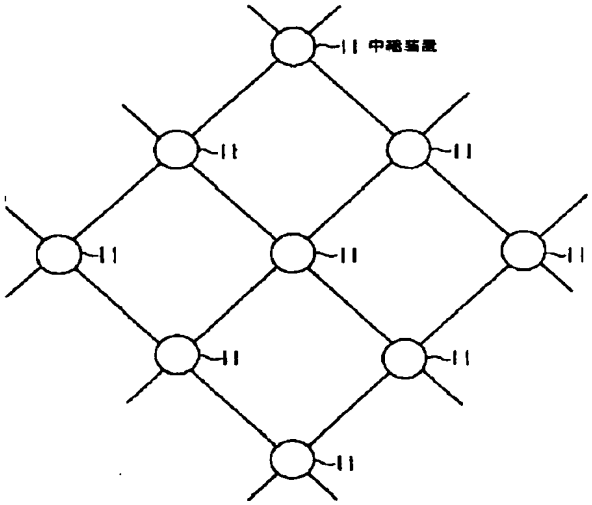
【図１】


11
中継装置
111
ポート
イネーブル
/ディス
エーブル
EN/DIS
EN/DIS
EN/DIS
EN/DIS
P1
P2
P3
P4
12
LANセグメント
13
LANセグメント
14
LANセグメント
15
LANセグメント
端末

【図２】


11
1
1B
2
4
4A
4B
1A
1D
2C
4B
P1
1A'
送受信
制御
3C
1B
4A
4B
1A
2A
3A
P2
1C
2B
3B
3C
4A
4B
1A
共通制御
1C
3C
P3
1B
1A
4B
P4
1C
3
中継装置

【図４】


11 中継装置
11
11
11
11
11
11
11